Министерство связи и массовых коммуникаций Российской Федерации

Государственное образовательное учреждение
высшего профессионального образования

ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ

ЭЛЕКТРОННАЯ БИБЛИОТЕЧНАЯ СИСТЕМА

Самара

ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
Государственное образовательное учреждение высшего профессионального образования
«Поволжский государственный университет телекоммуникаций и информатики»

Кафедра МСИБ

Методические разработки к лабораторным работам по дисциплине «Компьютерные сети»

«Изучение маршрутизации на базе оборудования Cisco»

для студентов специальностей 210406, 210400, 210403

Составители:
к.т.н., доц. Киреева Н. В.
к.т.н., доц. Криштофович А.Ю.
асс. Буранова М.А.

Редактор:
д.т.н., проф. Зайкин В.П.

Рецензент:
д.т.н., проф. Васин Н.Н.

Самара 2010

Лабораторная работа №1

Бесклассовая маршрутизация. IP - протокол

Цель работы: приобрести навыки в разделении сети на подсети с разными IP-адресами.

Рекомендуемые источники

1.Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3-е изд. – Спб.: Питер, 2006. - 958 с.: ил.

2.Столлингс В. Передача данных. - 4-е изд. Спб.: Питер, 2009.

3. Ричард Стивене. Протоколы TCP/1P. Практическое руководство. - Спб.: БХВ, 2003.

Общие сведения

Основные функции IP – протокола

Название протокола межсетевого взаимодействия (Internet Protocol) - отражает его суть: он должен передавать пакеты между сетями. В каждой очередной сети, лежащей на пути перемещения пакета, протокол IP вызывает средства транспортировки, принятые в этой сети, чтобы с их помощью передать этот пакет на маршрутизатор, ведущей к следующей сети, или непосредственно к узлу-получателю.

Протокол IP относится к протоколам без установления соединения. Перед ним не становится задача надежной доставки сообщений от отправителя к получателю. Протокол обрабатывает каждый пакет как независимую единицу, не имеющую связи ни с какими другими пакетами.

Важной особенностью протокола IP является его способность выполнять динамическую фрагментацию пакетов при передаче их между сетями с различными максимально допустимыми значениями длины поля данных кадров.

Использование масок для структуризации сети

Алгоритмы маршрутизации усложняется, когда в систему адресации узлов вносятся дополнительные элементы - маски. Часто администраторы сети испытывают неудобства из-за того, что количество централизованно выделенных им номеров сетей недостаточно для того, чтобы структурировать сеть надлежащим образом, например, разместить все слабо взаимодействующие компьютеры в разных сетях. В такой ситуации возможны два пути. Первый из них связан с получением от поставщика услуг Интернета дополнительных номеров сети. Второй способ связан с использованием

технологии масок, которая позволяет разделять одну сеть на несколько сетей. Допустим, администратор получил в свое распоряжение адрес 192.44.0.0. Он может организовать сеть с большим числом узлов, номера которых выбрать из диапазона 0.0.0.1 - 0.0.255.254. Однако ему не нужна одна большая неструктурированная сеть, производственная необходимость диктует администратору другое решение, в соответствии с которым сеть должна быть разделена на три отдельных подсети, при этом трафик в каждой подсети должен быть надежно локализирован. Это позволит легче диагностировать сеть и проводить в каждой из подсетей особую политику безопасности.

Номер сети, который администратор получил от поставщика услуг, - 129.44.0.0 (10000001 00101100 00000000 00000000). В качестве маски было выбрано значение 255.255.192.0 (11111111 11111111 11000000 00000000). После наложения маски на этот адрес число разрядов увеличилось с 16 (стандартная длина поля номера сети для класса B) до 18 (число единиц в маске), то есть администратор получил возможность использовать два дополнительных бита для нумерации подсетей. Это позволяет ему сделать из одного централизованно заданного ему номера сети четыре:

129.44.0.0 (10000001 00101100 00000000 00000000)
129.44.64.0 (10000001 00101100 01000000 00000000)
129.44.128.0 (10000001 00101100 1000000000000000)
129.44.192.0 (10000001 00101100 1100000000000000)

Технология бесклассовой маршрутизации

Из-за несовершенства протоколов маршрутизации обмен сообщениями об обновлении таблиц маршрутизации стал иногда приводить к сбоям магистральных маршрутизаторов из-за перегрузки при обработке большого объема служебной информации. На решение этой проблемы была направлена технология бесклассовой междоменной маршрутизации (Classless Inter Domain Routing, CIDR).

Каждому поставщику услуг Интернета должен назначаться непрерывный диапазон в пространстве IP-адресов. При таком подходе адреса всех сетей каждого поставщика услуг имеют общую старшую часть - префикс, поэтому маршрутизация на магистралях Интернета может осуществляться на основе префиксов, а не полных адресов сетей. Пусть поставщик услуг Интернета располагает пулом адресов в диапазоне 193.20.0.0 - 193.23.255.255 (1100 0001.0001 0100.0000 0000.0000 0000 - 1100 0001.0001 0111. 1111 1111.1111 1111) с общим префиксом 193.20 (1100 0001.0001 01) и маской, соответствующей этому префиксу 255.252.0.0. Если абоненту этого поставщика требуется совсем немного адресов, например, 13. то поставщик мог бы предложить ему различные варианты: сеть 193.20.30.0, сеть 193.20.30.16 или сеть 193.21.204.48, все с одним и тем же значением маски 255.255.255.240. Во

всех случаях в распоряжении абонента для нумерации узлов имеются 4 младших бита. Если к поставщику услуг обратился крупный заказчик и ему требуется блок адресов в 4000 узлов. На нумерацию такого количества пойдет 12 двоичных разрядов, следовательно, маска будет иметь значение 255.255.240.0 и размер выделенного пула адресов окажется несколько больше требуемого - 4096.

Пример.

Дана сеть с адресом 192.168.8.0/24. Необходимо разбить данную сеть на 3 подсети, в каждой из которых 6, 12, 54 компьютера. Маска заданной сети имеет вид 11111111.11111111.11111111.00000000, т.е. 255.255.255.0. Вычислим маску для подсети, в которой содержится 6 компьютеров. Учитывая, что два адреса используются на broadcast и широковещательный адрес, то минимальное количество адресов для данной подсети 5, значит $2^{2:}$-4 адреса, недостаточно, берем 2^3-8 адресов. Маска подсети будет иметь вид 255.255.255.248.

Аналогично, выполняя действия для двух других подсетей, получим: -для подсети на 12 хостов маску 255.255.255.240 -для подсети на 54 хоста маску 255.255.255.192

Результаты нарезки сети занесем в таблицу Таблица 1

	Подсети	Минимальный адрес узла	Максимальный адрес узла	Маска подсети
6	192.168.8.0	192.168.8.1	192.168.8.6	255.255.255.248
12	192.168.8.8	192.168.8.9	192.168.8.23	255.255.255.240
54	192.168.8.25	192.168.8.26	192.168.8.80	255.255.255.192

Содержание отчета

1. Цель работы.
2.Выполнение задания на лабораторную работу
3.Сводная таблица результатов по заданию.
4.Выводы по проделанной работе.

Задание на лабораторную работу

Дана сеть с адресом. Необходимо разбить данную сеть на 3 подсети, в каждой из которых определенное количество компьютеров. В соответствии с занимаемым рабочем местом варианты представлены в таблице 2

Таблица 2

№	Адрес сети	Количество хостов в сети
1	192.168.4.0/16	6/10/12
2	192.168.12.0/30	2/15/60
3	192.168.16.0/32	40/4/25
4	192.168.24.0/24	20/14/2
5	192.168.30/22	10/16/8
6	192.168.36/18.	15/23/58

Контрольные вопросы.

1.Назначение протокола IP.

2 Формат IP протокола.

3. Классы IP адресов.

4.Назначение масок в IP-адресах.

5.Какие проблемы при использовании IP-адресов решает бесклассовая маршрутизация?

6.Адрес узла 172.16.100.69, маска 255.255.0.0. Вычислить адрес сети.

7.Необходимо создать 30 подсетей, сколько компьютеров может быть в одной сети?

Лабораторная работа №2

Сетевой стек операционной системы Windows XP, стек TCP/IP

Цель работы: научиться настраивать IP-протокол в среде Windows XP

Рекомендуемые источники

1. Олифер В. Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3-е изд. - Спбю: Питер, 2006. -958 с.: ил.
2. Столлингс В. Передача данных. - 4-е изд. Спб.: Питер, 2004.
3. Кульгин С.Г. Сети TCP/IP.

Общие сведения

Протокол ICMP

IP протокол используется для обработки датаграммы, передаваемой между хост-компьютерами в системе объединенных сетей, называемой Catanet. Устройства, осуществляющие соединение различных сетей, называются шлюзами. Для обеспечения управления шлюзы общаются друг с другом посредством протокола Gateway to Gateway Protocol (GGP). Порой шлюз или хост-компьютер, получающий данные, обменивается информацией с хост-компьютером, отправляющим эти данные. Именно для таких целей используется данный протокол - протокол контрольных сообщений Intenet (ICMP). ICMP использует основные свойства IP протокола, как если бы ICMP являлся протоколом более высокого уровня. Однако фактически ICMP является составной частью IP протокола и должен являться составной частью каждого модуля IP.

Сообщения ICMP должны отправляться в некоторых затруднительных ситуациях. Например, когда датаграмма не может достичь своего адресата, когда шлюз не имеет достаточно места в своем буфере для передачи какой-либо датаграммы, или когда шлюз приказывает хост-компьютеру отправлять информацию по более короткому маршруту.

IP протокола не создан для того, чтобы обеспечивать абсолютную надежность передачи информации. Целью же данных контрольных сообщений является обеспечение обратной связи, оповещение отправителя данных о проблемах, возникающих в коммуникационном оборудовании. Их целью не является придание надежности IP протоколу. Протокол не дает гарантий, что датаграмма достигает своего адресата или что контрольное сообщение будет возвращено компьютеру, отправившему данные. Некоторые из датаграмм могут исчезнуть в сети, не вызвав при этом ни каких оповещений. Протоколы более высокого уровня, использующие IP протокол, должны применять свои собственные процедуры для обеспечения надежности передачи данных, если таковая требуется.

Сообщения ICMP протокола, как правило, оповещают об ошибках, возникающих при обработке датаграмм. Чтобы проблемы с передачей сообщений не вызывали появление новых сообщений, чтобы это в свою очередь не привело к лавинообразному росту количества сообщений, циркулирующих в сети, констатируется, что нельзя посылать сообщения о сообщениях. Также констатируется, что ICMP сообщения можно посылать только о проблемах, возникающих при обработке нулевого фрагмента в сегментированной датаграмме (нулевой фрагмент имеет нуль в поле смещения фрагмента).

Протокол ARP

Для определения локального адреса по IP адресу используется протокол разрешения адреса Address Resolution Protocol. Протокол АКР работает различным образом в зависимости от того, какой протокол канального уровня работает в данной сети - протокол локальной сети (Ethernet, Token Ring, FDDI) с возможностью широковещательного доступа одновременно ко всем узлам сети, или же протокол глобальной сети (X.25, Frame Relay), как правило не поддерживающий широковещательный доступ. Существует также протокол, решающий обратную задачу - нахождение IP адреса по известному локальному адресу. Он называется реверсивный ARP - RARP (Reverse Address Resolution Protocol) и используется при старте бездисковых станций, не знающих в начальный момент своего IP адреса, но знающих адрес своего сетевого адаптера.

В локальных сетях протокол ARP использует широковещательные кадры протокола канального уровня для поиска в сети узла с заданным IP адресом.

Узел, которому нужно выполнить отображение IP адреса на локальный адрес, формирует ARP запрос, вкладывает его в кадр протокола канального уровня, указывая в нем известный IP адрес, и рассылает запрос широковещательно. Все узлы локальной сети получают ARP запрос и сравнивают указанный там IP адрес с собственным. В случае их совпадения узел формирует ARP ответ, в котором указывает свой IP адрес и свой локальный адрес и отправляет его уже направленно, так как в ARP запросе отправитель указывает свой локальный адрес. ARP запросы и ответы используют один и тот же формат пакета. Так как локальные адреса могут в различных типах сетей иметь различную длину, то формат пакета протокола ARP зависит от типа сети.

В поле типа сети для сетей Ethernet указывается значение 1. Поле типа протокола позволяет использовать пакеты ARP не только для IP протокола, но и для других сетевых протоколов. Для IP значение этого поля равно 080016.

Длина локального адреса для протокола Ethernet равна 6 байтам, а длина IP адреса 4 байтам. В поле операции для ARP запросов указывается значение 1 для протокола ARP и 2 для протокола RARP.

Узел, отправляющий ARP запрос, заполняет в пакете все поля, кроме поля искомого локального адреса (для RARP-запроса не указывается искомый IP адрес). Значение этого поля заполняется узлом, опознавшим свой IP адрес.

В глобальных сетях администратору сети чаще всего приходится вручную формировать ARP таблицы, в которых он задает, например, соответствие IP адреса адресу узла сети X.25, который имеет смысл локального адреса. В последнее время наметилась тенденция автоматизации работы протокола ARP и в глобальных сетях. Для этой цели среди всех маршрутизаторов, подключенных к какой-либо глобальной сети, выделяется специальный маршрутизатор, который ведет ARP-таблицу для всех остальных узлов и маршрутизаторов этой сети. При таком централизованном подходе для всех узлов и маршрутизаторов вручную нужно задать только IP адрес и локальный адрес выделенного маршрутизатора. Затем каждый узел и маршрутизатор регистрирует свои адреса в выделенном маршрутизаторе, а при необходимости установления соответствия между IP адресом и локальным адресом узел обращается к выделенному маршрутизатору с запросом и автоматически получает ответ без участия администратора.

Протокол DHCP

Основным назначением DHCP является динамическое назначение IP адресов. Однако, кроме динамического, DHCP может поддерживать и более простые способы ручного и автоматического статического назначения адресов.

В ручной процедуре назначения адресов активное участие принимает администратор, который предоставляет DHCP серверу информацию о соответствии IP адресов физическим адресам или другим идентификаторам клиентов. Эти адреса сообщаются клиентам в ответ на их запросы к DHCP серверу.

При автоматическом статическом способе DHCP сервер присваивает IP адрес (и, возможно, другие параметры конфигурации клиента) из пула наличных IP адресов без вмешательства оператора. Границы пула назначаемых адресов задает администратор при конфигурировании DHCP сервера. Между идентификатором клиента и его IP адресом по-прежнему, как и при ручном назначении, существует постоянное соответствие. Оно устанавливается в момент первичного назначения сервером DHCP IP адреса клиенту. При всех последующих запросах сервер возвращает тот же самый IP адрес.

При динамическом распределении адресов DHCP сервер выдает адрес клиенту на ограниченное время, что дает возможность впоследствии повторно использовать IP адреса другими компьютерами. Динамическое разделение адресов позволяет строить IP сеть, количество узлов в которой намного превышает количество имеющихся в распоряжении администратора IP адресов.

DHCP обеспечивает надежный и простой способ конфигурации сети TCP/IP, гарантируя отсутствие конфликтов адресов за счет централизованного управления их распределением. Администратор управляет процессом назначения адресов с помощью параметра "продолжительности аренды" (lease

duration), которая определяет, как долго компьютер может использовать назначенный IP адрес, перед тем как снова запросить его от сервера DHCP в аренду.

Примером работы протокола DHCP может служить ситуация, когда компьютер, являющийся клиентом DHCP, удаляется из подсети. При этом назначенный ему IP адрес автоматически освобождается. Когда компьютер подключается к другой подсети, то ему автоматически назначается новый адрес. Ни пользователь, ни сетевой администратор не вмешиваются в этот процесс. Это свойство очень важно для мобильных пользователей.

Протокол UDP

UDP (User Datagram Protocol, протокол дейтаграмм пользователя) предназначен для обмена дейтаграммами между процессами компьютеров, входящих в единую сеть с коммутацией пакетов. В качестве протокола нижнего уровня UDP протокол использует IP.

Протокол UDP предоставляет прикладным программам возможность отправлять сообщения другим приложениям, используя минимальное количество параметров протокола. Этот протокол не обеспечивает достоверность доставки пакетов, защиты дублирования данных или надежности от сбоев в передаче. За исключением параметров приложения -номеров портов отправителя и получателя пакета, UDP практически ничего не добавляет к IP дейтаграмме.

Протокол UDP намного проще, чем TCP и полезен в ситуациях, когда мощные механизмы обеспечения надежности протокола TCP не требуются или будут только помехой для решения определенного рода задач, например, аутентификации пользователей.

Source Port (16 бит). Порт отправителя. Это поле может содержать номер порта, с которого был отправлен пакет, когда это имеет значение (например, отправитель ожидает ответа). Если это поле не используется, оно заполняется нулями.

Destination Port (16 бит). Порт назначения - порт компьютера, на который пакет будет доставлен. Lenght (16 бит). Поле длины. Длина (в байтах) этой дейтаграммы, включая заголовок и данные. (минимальное значение этого поля равно 8). Checksum (16 бит). Поле контрольной суммы. Контрольная сумма UDP пакета представляет собой побитное дополнение 16-битной суммы 16-битных слов (аналогично TCP). В вычислении участвуют: данные пакета, заголовок UDP пакета, псевдозаголовок (информация от IP протокола), поля выравнивания по 16-битной границе (нулевые).

Преимущество протокола UDP состоит в том, что он требует минимум установок и параметров для соединения двух процессов между собой. Этот протокол используется при работе Серверов Доменов (Name Servers), при работе протокола TFTP (Trivial File Transfer, тривиальный протокол передачи данных), работе с SNMP и построении систем аутентификации. Идентификатор UDP в IP-заголовке - число 17.

Содержание отчета

1 .Цель работы.
2.Задание и исходные данные.
3.Описание используемых утилит.
4.Выводы по проделанной работе.

Задание на лабораторную работу:

1. Получить автоматические адреса по заданию преподавателя.
2. Проверить правильность автоматических адресов.
3. С помощью утилиты ping проверить: обмен пакетами между соседними компьютерами; обмен пакетами между всеми компьютерами; обмен пакетами между компьютером и сервером (шлюз по умолчанию 10.0.0.1); обмен пакетами между компьютером и Yandex, ping yandex.ru (указать количество промежуточных хостов).
4. Поменять автоматические адреса на произвольные.
5. Выполнить пункт №3.
6. С помощью команды netstat просмотреть статистику: - для сетевых интерфейсов; для отображения активных и пассивных соединений.

Ход работы

1. После получения автоматических адресов проверить правильность прописания: *Пуск/ Настройка/ Панель управления/ Сетевые подключения/ Подключение по локальной сети/ Общие/ Свойства/ Протокол Интернета TCP/IP*.
2. Для того, чтобы воспользоваться утилитой ping заходим в командную *строку'.Пуск'Выполнить/Ввести имя программы: cmd/ Ок* и проверяем обмен пакетами.
3. Меняем автоматические адреса на произвольные по пути, прописанному в пункте 1 и проверяем обмен пакетами с помощью утилиты ping.
4. Просмотрим статистику с помощью команды *Пуск/ Выполнить /cmd/ Ок.*

Контрольные вопросы

1. Какое функциональное предназначение протокола ICMP?
2. Назначение ARP.
3. Что прописывается в ARP таблицах?
4. Что можно проверить с помощью утилиты ping?
5. Определение и назначение протокола TCP.
6. Определение и назначение протокола UDP.
7. Принципы статического и динамического распределения адресов протокола DHCP.

Лабораторная работа №3

Настройка IP-протокола на маршрутизаторе Cisco.

Цель работы: Овладеть основными навыками настройки IP-протокола на маршрутизаторе Cisco.

Рекомендуемые источники:

1.Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы, Учебник для вузов. 3-е изд. - Спбю: Питер, 2006. - 958 с.: ил.

2.Столлингс В. Передача данных. - 4-е изд. Спб.: Питер, 2004.

3.Кульгин М.В. Сети TCP/IP.

Общие сведения

1.Протокол TELNET.

Протокол TELNET позволяет обслуживающей машине рассматривать все удаленные терминалы как стандартные "сетевые виртуальные терминалы" строчного типа, работающие в коде ASCII, а также обеспечивает возможность согласования более сложных функций (например, локальный или удаленный эхо-контроль, страничный режим, высота и ширина экрана и т.д.) TELNET работает на базе протокола TCP. На прикладном уровне над TELNET находится либо программа поддержки реального терминала (на стороне пользователя), либо прикладной процесс в обслуживающей машине, к которому осуществляется доступ с терминала. Работа с TELNET походит на набор телефонного номера. Пользователь набирает на клавиатуре что-то вроде Telnet Delta и получает на экране приглашение на вход в машину Delta.

Принципы построения

Протокол TELNET строится на базе TCP протокола и работает по дуплексному, многопользовательскому протоколу. Это значит, что один сервер может обслуживать одновременно несколько клиентов. Telnet построен на трех основных принципах:

1.NVT - Netvork Virtual Terminal - Принцип виртуальных терминалов. После установления соединения предполагается, что каждый участник работает как «Виртуальный сетевой терминал» - мнимое устройство, выполняющее стандартные сетевые промежуточные функции обычного терминала.

2.Принцип настраиваемых параметров. Если хост предоставляет дополнительный сервис помимо NVT, и клиент в состоянии его использовать, Telnet предоставляет возможность сделать это.

3.Принцип симметрии терминалов и процессов. Участники соединения равноправны.

Программы-клиенты

Работа с TELNET возможна и с помощью программ-клиентов, функционирующих под операционными системами DOS и Microsoft Windows. Один из примеров - free-пакет NCSA Telnet для DOS или HyperTerminal для Windows. Hyper Terminal - это специальное приложение Windows, позволяющее

устанавливать соединение с удаленным компьютером по коммутируемым телефонным линиям при помощи модема или нуль-модемного соединения, а также используемое в качестве основного клиента Telnet в среде Windows. Hyper Terminal может также применяться для подключения к удаленным сервисным службам и доскам объявлений (BBS).

VLAN. Общие понятия

VLAN (Virtual Local Area Network) — виртуальная локальная компьютерная сеть, представляет собой группу хостов с общим набором требований, которые взаимодействуют так, как, если бы они были подключены к широковещательному домену, независимо от их физического местонахождения. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным станциям группироваться вместе, даже если они не находятся в одной физической сети. Такая реорганизация может быть сделана на основе программного обеспечения вместо физического перемещения устройств. По умолчанию на каждом порту коммутатора имеется сеть VLAN1, необходимая для управления. Сеть управления не может быть удалена, однако могут быть созданы дополнительные сети VLAN и этим альтернативным VLAN могут быть дополнительно назначены порты.

Виртуальные локальные сети могут перекрываться, если один или несколько компьютеров входят в состав более чем одной виртуальной сети. Говорят, что виртуальная сеть образует домен широковещательного трафика, по аналогии с доменом коллизий, который образуется повторителями сетей Ethernet.

Содержание отчета

1. Цель работы.
2. Задание и исходные данные.
3. Описание используемых команд.
4. Выводы по проделанной работе.

Задание на лабораторную работу

1. Получить адрес сети у преподавателя.
2. Произвести подключение на патч-панели.
3. Создать VLAN на компьютерах.
4. Создать виртуальный интерфейс и прописать на нем IP-адрес.
5. С помощью команды ping проверить обмен информацией между компьютером и маршрутизатором.

Ход работы

1. Произвести подключение на патч-панели, согласно предоставленной схеме подключения.

2. После получения адресов произвести настройку сетевого подключения. Для этого необходимо выбрать пункт меню Пуск, затем: *Настройка/Панель управления/Сетевые подключения/Подключение по локальной сети/Общие/Свойства/Протокол Интернета TCP/IP*. Изменяем IP адрес.

3. Для запуска HyperTerminal выбираем:

Пуск/Программы/Стандартные/Связь/HyperTerminal/Новое подключение(вводим любое имя)/Подключение/Com/Свойства/скорость 9600.

COM-порт указывается преподавателем. Имя и пароль по умолчанию *Cisco*.

Примечание: для подключения к маршрутизатору необходимо в окне HyperTerminal ввести команду *enable.*

4. Создаем VLAN. Для этого вводим последовательно команды: *vlan database/vlan2.* После создания VLAN выходим в основное меню при помощи команды *exit.* Просмотр созданной VLAN осуществляется командой: *show vlan-switch.*

5. Создаем интерфейс и назначаем ему IP-адрес в режиме конфигурирования. Вход в режим конфигурирования осуществляется командой *config t.* Затем вводим команды *int fast (номер интерфейса)/switchport access vlan 2* (добавляет в vlan 2 выбранный интерфейс).

Примечание: номер интерфейса выбирается в соответствии со схемой.

Выходим из режима конфигурирования командой *exit.*

6. С помощью команды *show interface vlan 2* просматриваем прописанный IP-адрес. Этот IP-адрес необходимо заменить на адрес, полученный у преподавателя. Для этого входим в режим конфигурирования (*config t)* и вводим команду*: int vlan 2.* Удаляем исходный IP-адрес: *no ip address (напр., no ip address 192.168.7.1 255.255.255.248)* для того, чтобы убедиться в удалении исходного IP-адреса выходим из режима конфигурирования (*exit*) и вводим команду: *show int vlan2.* Если исходный адрес успешно удален, то назначаем новый IP-адрес. В режиме конфигурирования вводим команду *int vlan2* и прописываем адрес, полученный у преподавателя, с помощью команды: *ip address (адрес с маской).* С помощью команды *show int vlan 2* (выйти из режима конфигурирования) убедимся, что новый адрес прописан

7. Проверим правильность выполненных действий с помощью команды *ping (вводим IP-адрес VLAN, напр.: ping 172.163.50.2).* Следует обратить внимание, что данная проверка проводилась со стороны маршрутизатора. Если проверка выполнена успешно, то произведем проверку со стороны компьютера. Для этого выбираем: *Пуск/Выполнить/cmd/Ок/ping(адрес VLAN).*

Контрольные вопросы

1. Назначение протокола Telnet.
2. Три основных принципа протокола Telnet.
3. Назначение VLAN, принципы ее создания.
4. Назначение команды ping.
5. Назначение команды *show interface vlan.*
6. NVT - Netvork Virtual Terminal принцип работы.

Лабораторная работа №4

Конфигурирование статической маршрутизации

Цель работы: изучения процесса пересылки пакетов из одной сети в другую и доставки их в узлы назначения с помощью статической маршрутизации.

Задание на лабораторную работу
1. Создать VLAN и назначить ей IP-адрес с маской.
2. Сконфигурировать маршрутизацию для каждого маршрутизатора.
3. Проверить создание конфигурации
4. Проверить обеспечение IP-связи между маршрутизаторами.
5. Проверить таблицу маршрутизации.

Содержание отчета:
1.Название лабораторной работы;
2.Цель работы;
3.Задание;
4.Ход работы;
5.Ответы на контрольные вопросы.

Общие сведения

Маршрутизация - это процедура определения пути следования пакета между сетями. Маршрутизация включает в себя два основных компонента: определение оптимальных трактов маршрутизации и транспортировка пакетов через объединенную сеть.

Статическая IP-маршрутизация является функцией IP. Это значит, что маршрутизаторы не обмениваются информацией о маршрутах автоматически. Статический маршрут может быть определен путем назначения шлюза по умолчанию или в виде записи в таблице конфигурации. Наиболее стандартной настройкой является настройка маршрутизатора на использование статической маршрутизации. При этом сценарии вы сообщаете маршрутизатору обо всех подсетях, включая информацию об адресах для следующей пересылки. Заметьте, что маршрутизатор будет знать обо всех сетях и подсетях, к которым он присоединен сетевыми картами, поэтому у вас нет необходимости добавлять эту информацию в статическую таблицу маршрутизации, используя статические маршруты. Но для всех подсетей, к которым маршрутизатор не подключен непосредственно, вы обязательно должны вносить информацию в таблицу маршрутизации. Добавление большого количества маршрутов вызывает дополнительные трудности, поэтому, во многих случаях, предпочтительным является использование протоколов маршрутизации. Однако, статическая маршрутизация предоставляет наиболее быстрый, простой

и эффективный метод для настройки маршрутизации, особенно в небольших сетях.

В корпоративной сети, имеющей, хотя бы один статический маршрутизатор, необходимо сконфигурировать записи статической таблицы маршрутизации для всех известных сетей на каждом маршрутизаторе.

Запись статической таблицы маршрутизации создана на компьютере A. Она содержит идентификатор сети 3 и IP-адрес интерфейса (131.107.16.1), к которому компьютер A имеет прямой доступ и который может перенаправлять пакеты из сети 1 в сеть 3. Запись статической таблицы маршрутизации создана на компьютере B. Запись содержит сетевой идентификатор сети 1, а также IP-адрес интерфейса (131.107.16.2), который напрямую доступен компьютеру B для того, чтобы перенаправлять пакеты из сети 3 в сеть 1.

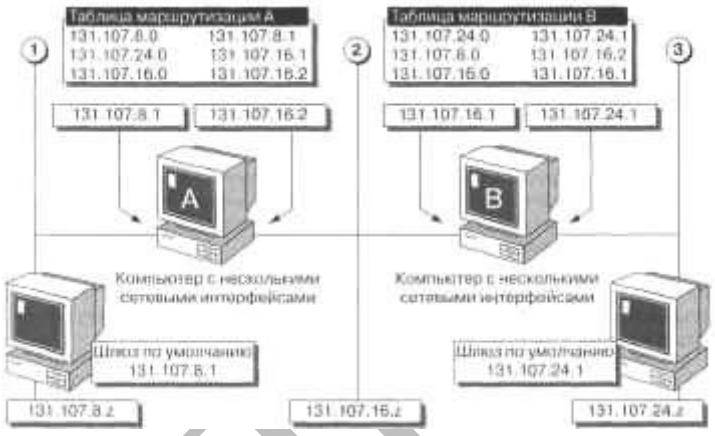

Рисунок 1-Конфигурирование статических IP-маршрутизаторов

Если в корпоративной сети более двух маршрутизаторов и по крайней мере один из них является статическим, Вам необходимо сконфигурировать статическую таблицу маршрутизации на каждом компьютере с несколькими сетевыми интерфейсами. Для того, чтобы компьютер мог соединиться с другими в корпоративной сети, в его конфигурации адрес шлюза по умолчанию должен соответствовать IP-адресу локального интерфейса маршрутизатора.

Использование адреса шлюза по умолчанию

Существует несколько методов конфигурирования статического маршрута без ручного добавления маршрутов в таблицу. Один из них — задать в качестве адреса шлюза по умолчанию для каждого компьютера с несколькими сетевыми интерфейсами адрес локального интерфейса другого компьютера с несколькими сетевыми интерфейсами в той же сети. Этот метод эффективен только в случае двух статических маршрутизаторов.

Ход работы

1. Создаем VLAN на каждом маршрутизаторе, аналогично предыдущей работе. Создание VLAN необходимо для назначения IP адресов и подключения к ним интерфейсов. Интерфейсы выбираются согласно схеме.

Примечание: Для второго маршрутизатора нужно создать две VLAN.

2. Используем команду *ip route*, чтобы сконфигурировать статическую маршрутизацию. Затем указываем адрес присоединенной сети, маску и адрес шлюза непосредственно присоединенного маршрутизатора. Например:

Маршрутизатор А связан с сетями 192.168.8.0 и 192.168.7.0, а статическая маршрутизация должна создаваться для каждой сети, которая непосредственно не присоединяется.

A#config t ;

A(config t)#ip route 192.168.8.0 255.255.255.248 192.168.8.2;

A(config t)#ip route 192.168.7.0 255.255.255.248 192.168.7.1;

A(config t)# exit;

Аналогично используем команду *ip route* для двух других маршрутизаторов.

3. Для проверки создания конфигурации используется команда *show ip route.*

4. После проверки маршрутизации во всех маршрутизаторах используем команду *ping*, чтобы проверить связь между маршрутизаторами.

5. Конфигурация по умолчанию статической маршрутизации. Для конфигурации маршрутизации по умолчанию используем команду *ip route*, но вместо маски сети и подсети используем все нули, которые означает все сети и все маски *(ip route 0.0.0.0 0.0.0.0 192.168.8.1).*

6. Проверим таблицу маршрутизации по умолчанию используя команды *show ip route* и *ping*.

Контрольные вопросы.

1. Что такое статическая маршрутизация?
2. Назначение команды *ip route.*
3. Как осуществит просмотр таблицы маршрутизации?
4 Отличие записи команды ip route при маршрутизации по умолчанию.
5. Каким образом конфигурируется статическая маршрутизация.

Рекомендуемые источники:

1.Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3-е изд. - Спб: Питер, 2006. - 958 с.: ил.

2. Столлингс В. Передача данных. - 4-е изд. Спб.: Питер, 2004.

3. Ричард Стивенс. Протоколы TCP/IP. Практическое руководство. – Спб.: БХВ, 2003.

Лабораторная работа № 5

Динамическая маршрутизация на основе протокола RIP

Цель работы: приобрести навыки в работе с динамической маршрутизацией на основе протокола RIP.

Задание на лабораторную работу

Дана сеть с адресом, на которой необходимо настроить протокол RIP, после чего проверить правильность производимого конфигурирования. Исходные данные предложены в таблице 3.2. Номер варианта соответствует номеру занимаемого рабочего места в лаборатории.

Исходные данные

Номер варианта	Адрес сети маршрутизатора	Адрес сети компьютера
1	192.168.63.0	173.156.43.0
2	163.128.45.0	198.163.7.0
3	172.126.78.0	183.113.34.0

Содержание отчета:

1. Название лабораторной работы;
2. Цель работы;
3. Задание;
4. Ход работы;
5. Ответы на контрольные вопросы.

Общие сведения:

Протокол RIP является дистанционно-векторным протоколом внутренней маршрутизации. Процесс работы протокола состоит в рассылке, получении и обработке векторов расстояний до IP-сетей, находящихся в области действия протокола, то есть в данной RIP-системе. Результатом работы протокола на конкретном маршрутизаторе является таблица, где для каждой сети данной RIP-системы указано расстояние до этой сети (в хопах) и адрес следующего маршрутизатора.

Протокол RIP очень прост и до сих пор продолжает использоваться в системах с простой топологией, но обладает недостатками, которые не позволяют применять его в обширных и сложных системах. Во-первых, малое значение бесконечности (из-за эффекта "счет до бесконечности") ограничивает размер RIP-системы четырнадцатью промежуточными маршрутизаторами в любом направлении. Кроме того, по той же причине весьма затруднительно использование сложных метрик, учитывающих не просто количество промежуточных маршрутизаторов, но и скорость и качество канала связи (чем медленнее канал, тем больше метрика). Во-вторых, само явление счета до бесконечности вызывает сбои в маршрутизации. В-третьих,

широковещательная рассылка векторов расстояний каждые 30 секунд ухудшает пропускную способность сети. В-четвертых, время схождения алгоритма при создании маршрутных таблиц достаточно велико (по крайней мере, по сравнению с протоколами состояния связей). В-пятых, несмотря на то, что каждый маршрутизатор начинает периодическую рассылку своих векторов, через некоторое время в системе наблюдается эффект синхронизации маршрутизаторов, сходный с эффектом синхронизации аплодисментов. Все маршрутизаторы рассылают свои вектора в один и тот же момент времени, что приводит к большим пикам трафика и отказам в маршрутизации дейтаграмм во время обработки большого количества одновременно полученных векторов.

Протокол маршрутизации Routing Information Protocol (RIP) для IP облегчает обмен информацией о маршрутизации в объединенной IP-сети. RIP позволяет маршрутизаторам обмениваться идентификаторами сетей (network IDs), которых может достичь маршрутизатор, и расстоянием до этих сетей. RIP использует поле подсчета транзитов (hop count), или метрику (metric), в своей таблице маршрутизации для отображения расстояния до сети, обозначенной соответствующим идентификатором. Количество транзитов — это число маршрутизаторов, которые должны быть пройдены для достижения требуемого идентификатора сети. Максимальное количество транзитов для RIP-записи равно 15. Сетевые идентификаторы, требующие 16 и более транзитов, считаются недостижимыми. Количество транзитов может быть изменено для отображения медленных или перегруженных каналов. Если в таблице маршрутизации несколько записей для одного сетевого идентификатора, то RIP-маршрутизатор выберет маршрут с наименьшим числом транзитов.

Динамическая маршрутизация на малых сетях очень проста. Важно отметить, что сетевой адрес является адресом с кластером (classful). Это означает, что в RIP-протоколе нельзя использовать сети класса В (172.16.0.0) и подсети с 24-битными масками, то есть когда третий октет используется для адресации подсетей, а четвертый – для адресации узлов каждой сети. RIP – протокол маршрутизации типа classful, означающий, что можно только использовать адреса класса В.маршрутизации RIP.

Протокол RIP-2 (RFC-1388, 1993 год) является новой версией RIP, которая в дополнение к широковещательному режиму поддерживает мультикастинг; позволяет работать с масками субсетей.

Ход работы

1. Конфигурируя RIP, необходимо сначала создать VLAN для каждой сети и прописать на них IP-адреса согласно варианту. Затем подключить на них интерфейсы, в соответствии со схемой.

2. Войти в режим конфигурирования командой *config t.* Сконфигурировать протокол RIP, используя команду *router rip.*

3. На маршрутизаторе R1 сконфигурировать RIP и сообщить протоколу RIP адреса всех сетей. Например:

R1#(config t)
R1(config)#router rip
R1(config-router)# network 172.128.32.0
R1(config-router)# network 192.178.56.0
R1(config-router)# exit

4. На маршрутизаторе R1 используем команду *show ip router*, чтобы просмотреть таблицу маршрутизации. Символом R обозначен маршрут, найденный протоколом RIP. Символом C – непосредственно подсоединенная сеть.

Примечание: На маршрутизаторе R1 изменить версию протокола RIP. Это осуществляется в режиме конфигурирования:

R1#(config t)
R1(config)#router rip
R1(config-router)# version 1
R1(config-router)# exit

4. Аналогично на других маршрутизаторах сконфигурировать протокол RIP и сообщить протоколу RIP адреса сетей.

5. Проверить правильность конфигурации командой *ping*. Если всё верно, то все адреса, входящие в объявленные сети будут пинговаться.

Контрольные вопросы:

1. Протокол RIP. Его функции и назначение.
2. Основные недостатки протокола.
3. Какая команда используется для просмотра таблицы маршрутизации?
4. Количество транзитов, каково их число по умолчанию в протоколе RIP?
5. В чем отличие версий протокола RIP?

Лабораторная работа № 6

Динамическая маршрутизация на основе протокола OSPF

Цель работы: приобрести навыки работы с динамической маршрутизацией на основе протокола OSPF.

Содержание отчета

1. Цель, наименование работы;
2. Исходные данные по вариантам;
3. Описание используемых команд;
4. Порядок выполнения конфигурирования;
5. выводы по проделанной работе.

Общие сведения

Протокол OSPF (Open Shortest Path First — выбор кратчайшего пути первым) является достаточно современной реализацией алгоритма состояния связей и обладает многими особенностями, ориентированными на применение в больших гетерогенных сетях. OSPF разбивает процесс построения таблицы маршрутизации на два этапа.

На первом этапе каждый маршрутизатор строит граф связей сети, в котором вершинами графа являются маршрутизаторы и IP-сети, а ребрами — интерфейсы маршрутизаторов. Все маршрутизаторы для этого обмениваются со своими соседями той информацией о графе сети, которой они располагают к данному моменту. Этот процесс похож на процесс распространения векторов расстояний до сетей в протоколе RIP, однако сама информация качественно иная — это информация о топологии сети. Кроме того, при передаче топологической информации OSPF маршрутизаторы ее не модифицируют, как это делают RIP-маршрутизаторы, а передают в неизменном виде. В результате все маршрутизаторы сети располагают идентичными сведениями о графе сети, которые хранятся в базе данных о топологии сети.

Второй этап состоит в нахождении оптимальных маршрутов с помощью полученного графа. Задача нахождения оптимального пути на графе является достаточно сложной и трудоемкой, В протоколе OSPF для ее решения используется итеративный алгоритм Дийкстры. Каждый маршрутизатор считает себя центром сети и ищет оптимальный маршрут до каждой известной ему сети. В каждом найденном таким образом маршруте запоминается только один шаг — до следующего маршрутизатора, и соответствии с принципом одношаговой маршрутизации. Данные об этом шаге и попадают в таблицу маршрутизации. Если несколько маршрутов имеют одинаковую метрику до сети назначения, то в таблице маршрутизации запоминаются первые шаги всех этих маршрутов.

Для того чтобы база данных о топологии сети соответствовала текущему состоянию сети, OSPF -маршрутизаторам необходимо постоянно отслеживать

изменения состояния сети и вносить при необходимости коррективы в таблицу маршрутизации. Для контроля состояния связей и соседних маршрутизаторов OSPF-маршрутизаторы регулярно передают друг другу сообщения HELLO. Сообщения HELLO отправляются через каждые 10 секунд, чтобы повысить скорость адаптации маршрутизаторов к изменениям, происходящим в сети. Небольшой объем этих сообщений делает возможной такое частое тестирование состояния соседей и связей с ними. На основании принимаемых от непосредственных соседей сообщений HELLO маршрутизатор формирует записи о состоянии связях со своими непосредственными соседями и базе данных о топологии сети.

Характеристики протокола OSPF

1. Link-state протокол. Сообщения, с помощью которых распространяется топологическая информация, называются объявлениями о состоянии связей сети (Link State Advertisements, LSA).

2. VLSM - Variable Length Subnet Mask. В данном протоколе отменяются классы маршрутизации, так как простая схема с сетями класса A,B,C недостаточно гибка,требуется чтобы протоколы роутинга умели поддерживать VSML. OSPF решает эту задачу.

3. Расчитан для работы в иерархических сетях.

4. Разделние сети на отдельные области (Areas) Область это группа смежных сетей. Области представляют собой логические разделы автономной системы. Если в протоколе OSPF используются области, сетью становится проще управлять и наблюдается заметное сокращение трафика маршрутизации. Эти преимущества достигаются благодаря тому, что топология области становится невидимой для других маршрутизаторов, находящихся за пределами этой области. Области позволяют также находящимся в них маршрутизаторам иметь свою базу данных о состоянии каналов и применять алгоритм SPF.

5. Поддерживается роутерами большинства производителей.

Классификация OSPF роутеров

1. Area Border Router (ABR) — Пограничный маршрутизатор области. Имеет интерфейсы, подключенные сразу к нескольким областям. Для каждого из таких интерфейсов маршрутизирует трафик, направленный в другие области или прибывающий из них.

2. Internal router. Внутренний маршрутизатор. Имеет данные о топологии областей, в которых он находится, и ведет одинаковые базы данных состояния каналов для этих областей.

3. Backbone router. Магистральный маршрутизатор. Обеспечивает соединение областей.

4. Autonomous System Boundary router. Пограничный маршрутизатор автономной системы. Обменивается информацией с маршрутизаторами, принадлежащими разным автономным системам.

Задание на лабораторную работу:

Дана сеть с адресом. Необходимо настроить маршрутизацию на основе протокола OSPF, после чего проверить правильность производимого конфигурирования. Исходные данные предложены в таблице 1. Номер варианта соответствует номеру занимаемого рабочего места в лаборатории.

Таблица 1

№	Адрес сети
1	192.168.4.0/16
2	192.168.12.0/30
3	192.168.16.0/32

Ход работы

1. Конфигурируя OSPF, сначала необходимо удалить статические и заданные по умолчанию маршруты, сконфигурированные на маршрутизаторах.

2. Создаем VLAN аналогично предыдущим работам. Согласно схеме осуществляем подключение на них интерфейсов. используя команду, *switchport access* в режиме конфигурирования.

3. После создания VLAN настраиваем OSPF. Для этого входим в режим конфигурирования (*config t*), прописываем команду *router ospf 1*(где цифра обозначает номер запущенного OSPF процесса и одинакова для всех маршрутизаторов)

4. Вводим адреса сетей с инверсной маской и указанием идентификатора зоны. Важно, чтобы эти идентификаторы были одинаковыми для всех вариантов. Пример:

R1#(config t)
R1(config)#router ospf 1
R1(config-router)# network 192.168.8.0 0.0.0.7 area 0
R1(config-router)# network 172.168.50.0 0.0.0.7 area 0
R1(config-router)# exit

5. Для того, чтобы оценить состояние линка, используется команда *show ip ospf database*. Результат имеет примерный вид:

Router# show ip ospf database
OSPF Router with id(192.168.239.66) (Autonomous system 300)
Displaying Router Link States(Area 0.0.0.0)

Link ID	*ADV Router*	*Age*	*Seq#*	*Checksum*	*Link count*
172.18.21.6	*172.18.21.6*	*1731*	*0x80002CFB*	*0x69BC*	*8*
172.18.21.5	*172.18.21.5*	*1112*	*0x800009D2*	*0xA2B8*	*5*
172.18.1.2	*172.18.1.2*	*1662*	*0x80000A98*	*0x4CB6*	*9*
172.18.1.1	*172.18.1.1*	*1115*	*0x800009B6*	*0x5F2C*	*1*
172.18.1.5	*172.18.1.5*	*1691*	*0x80002BC*	*0x2A1A*	*5*

Displaying Net Link States(Area 0.0.0.0)

Link ID ADV Router Age Seq# Checksum
172.18.1.3 192.20.239.66 1245 0x800000EC 0x82E
Displaying Summary Net Link States(Area 0.0.0.0)
Link ID ADV Router Age Seq# Checksum
172.18.240.0 172.18.241.5 1152 0x80000077 0x7A05
172.18.241.0 172.18.241.5 1152 0x80000070 0xAEB7

Контрольные вопросы:

1. В чем заключается особенности протокола OSPF?
2. Какая команда выводит листинг с временами последний обновлений?
3. По какому принципу организуются адреса в OSPF?
4. Классификация OSPF маршрутизатора.